

# VAN LAMBALGEN’S THEOREM FOR UNIFORMLY RELATIVE SCHNORR AND COMPUTABLE RANDOMNESS

KENSHI MIYABE AND JASON RUTE

**ABSTRACT.** We correct Miyabe’s proof of van Lambalgen’s Theorem for truth-table Schnorr randomness (which we will call uniformly relative Schnorr randomness). An immediate corollary is one direction of van Lambalgen’s theorem for Schnorr randomness. It has been claimed in the literature that this corollary (and the analogous result for computable randomness) is a “straightforward modification of the proof of van Lambalgen’s Theorem.” This is not so, and we point out why. We also point out an error in Miyabe’s proof of van Lambalgen’s Theorem for truth-table reducible randomness (which we will call uniformly relative computable randomness). While we do not fix the error, we do prove a weaker version of van Lambalgen’s Theorem where each half is computably random uniformly relative to the other.

## 1. INTRODUCTION

Recall van Lambalgen’s theorem.

**Theorem 1.1** (van Lambalgen [13]).  *$A \oplus B$  is Martin-Löf random if and only if  $A$  is Martin-Löf random and  $B$  is Martin-Löf random relative to  $A$ .*

Merkle et al. [7] showed that the “ $\Rightarrow$ ” direction of van Lambalgen’s theorem does not hold for Schnorr or computable randomness. This has been extended by Yu [14], Kjos Hanssen [10, Remark 3.5.22], Franklin and Stephan [4], and Miyabe [9].

In [9] the first author claimed that van Lambalgen’s theorem does in fact hold for Schnorr randomness if the usual notion of relativized Schnorr randomness is replaced with the weaker notion of uniformly relative Schnorr randomness—previously called truth-table Schnorr randomness in [3] and [9].

**Theorem 1.2.**  *$A \oplus B$  is Schnorr random if and only if  $A$  is Schnorr random and  $B$  is Schnorr random uniformly relative to  $A$ .*

However, the proof given was incorrect and we provide a corrected proof. Our proof follows a standard proof of van Lambalgen’s theorem using integral tests, except at the difficult point we apply a Key Lemma, which can be seen as an effective version of Lusin’s theorem for a particular setting. Lusin’s theorem, one of Littlewood’s three basic principles of measure

theory, is the basis behind the layerwise-computability framework that has been successively employed by Hoyrup, Rojas and others to relate algorithmic randomness and computable analysis.

The structure of the paper is as follows. In Section 2, we prove the Key Lemma and some corollaries.

In Section 3, as a warm-up, we show how our Key Lemma can be used to prove the “ $\Leftarrow$ ” direction of van Lambalgen’s theorem for Schnorr randomness. (A different proof was given recently by Franklin and Stephan [4].) Yu [14] had claimed that “the [ $\Leftarrow$ ] direction of van Lambalgen’s theorem is true for both Schnorr randomness and computable randomness. [...] The proof is just a straightforward modification of the proof of van Lambalgen’s Theorem.” Downey and Hirschfeldt [2] had made similar claims. Unfortunately, the proofs are not so straightforward, and we explain why in the case of Schnorr randomness.

In Section 4, we define uniformly relative Schnorr randomness, and prove van Lambalgen’s theorem for this notion of randomness.

In Section 5, we discuss uniformly relative computable randomness—previously called truth-table reducible randomness. We remark that Miyabe’s [9] proof of van Lambalgen’s theorem for uniformly relative computable randomness is not correct in the “ $\Leftarrow$ ” direction. While we do not provide a correction, we do prove the following weaker result.

**Theorem 1.3.**  *$A \oplus B$  is computably random if and only if each of  $A$  and  $B$  are computably random uniformly relative to the other.*

This weakening of van Lambalgen’s theorem is also known to hold for Kolmogorov-Loveland randomness. We leave as an open question the “ $\Leftarrow$ ” direction of van Lambalgen’s theorem for both computable randomness and uniformly relative computable randomness. We conjecture that it is false for both.

Finally, in Section 6 we prove that Franklin and Stephan’s [3] truth-table Schnorr randomness is equivalent to our uniformly relative Schnorr randomness. The difference in terminology reflects the difference in definitions, and we discuss why the Franklin and Stephan definition, which uses truth-table reducibility, is very sensitive to the choice of test used.

## 2. THE KEY LEMMA

For this paper, we will work in  $2^\omega$  with the fair-coin measure  $\mu$ . Recall the following definitions. The reader may wish to consult the books [2, 10] for further background.

**Definition 2.1.** A *Martin-Löf test* is a uniform sequence  $\langle U_n \rangle$  of  $\Sigma_1^0$  subsets of  $2^\omega$  such that  $\mu(U_n) \leq 2^{-n}$ . A *Schnorr test* is a Martin-Löf test  $\langle U_n \rangle$  such that  $\mu(U_n)$  is uniformly computable in  $n$ . A set  $X \in 2^\omega$  is said to be *covered by* a Martin-Löf (Schnorr) test  $\langle U_n \rangle$  if  $X \in \bigcap_n U_n$ .  $X \in 2^\omega$  is said to be *Martin-Löf* (resp. *Schnorr*) *random* if  $X$  is not covered by any Martin-Löf (resp. Schnorr) test.

**Definition 2.2.** A function  $f: 2^\omega \rightarrow [0, \infty]$  is **lower semicomputable** if there is a uniform sequence of total computable functions  $g_n: 2^\omega \rightarrow [0, \infty)$  such that  $f = \sum_n g_n$ .

A more standard definition of lower semicomputable is that  $f$  is lower-semicomputable if  $f(X)$  is uniformly lower-semicomputable (left c.e.) from  $X$ . Our definition is easily seen to be equivalent. (This even remains true when  $2^\omega$  is replaced with the unit interval or another computable Polish space.)

Recall the following definitions.

**Definition 2.3.** A function  $f: 2^\omega \rightarrow \mathbb{R}$  is  **$L^1$ -computable** if it can be effectively approximated by bounded computable functions in the  $L^1$ -norm. (Since  $2^\omega$  is compact, all computable functions are bounded.)

The **distribution** of a function  $f: 2^\omega \rightarrow \mathbb{R}$  is the probability measure  $\nu$  on  $\mathbb{R}$  defined by  $\nu(A) = \mu(\{X \in 2^\omega : f(X) \in A\})$  for all Borel sets  $A \subseteq \mathbb{R}$ .

A distribution  $\nu$  is **computable** if  $\nu(U)$  is lower semicomputable (left c.e.) uniformly from the code for an open set  $U$ .

We could not find a direct proof of this next fact, so we give one here.

**Proposition 2.4.** *Let  $f: 2^\omega \rightarrow \mathbb{R}$  be an  $L^1$ -computable function with distribution  $\nu$ . Then  $\nu$  is a computable distribution.*

*Proof.* It is enough to prove that

$$\nu((a - r, a + r)) = \mu(\{X \in 2^\omega : |f(X) - a| < r\})$$

is lower semicomputable from  $a, r$ .

If  $f$  is computable, then we are done, since  $\{X \in 2^\omega : |f(X) - a| < r\}$  is  $\Sigma_1^0$  relative to  $a$  and  $r$ .

Otherwise, we know

$$(1) \quad \begin{aligned} & \mu(\{X \in 2^\omega : |f(X) - a| < r\}) \\ &= \sup_{\varepsilon > 0} \mu(\{X \in 2^\omega : |f(X) - a| < r - \varepsilon\}). \end{aligned}$$

For any  $\varepsilon > 0$  and  $\delta > 0$  we can effectively approximate  $f$  by some computable function  $g$  such that  $\|f - g\|_{L^1} < \varepsilon \cdot \delta$ . Then by Chebeshev's inequality,

$$\mu(\{X \in 2^\omega : |f(X) - g(X)| \leq \varepsilon\}) \leq (\varepsilon \cdot \delta) / \varepsilon = \delta.$$

So outside a set of measure at most  $\delta$ , we have  $|f(X) - g(X)| < \varepsilon$ , and therefore

$$|f(X) - a| < r - 2\varepsilon \quad \Rightarrow \quad |g(X) - a| < r - \varepsilon \quad \Rightarrow \quad |f(X) - a| < r.$$

Expressing this with measures gives us

$$\begin{aligned} \mu(\{X \in 2^\omega : |f(X) - a| < r\}) &\geq \mu(\{X \in 2^\omega : |g(X) - a| < r - \varepsilon\}) - \delta \\ &\geq \mu(\{X \in 2^\omega : |f(X) - a| < r - 2\varepsilon\}) - 2\delta. \end{aligned}$$

Combining this with (1) we get

$$\begin{aligned} \mu(\{X \in 2^\omega : |f(X) - a| < r\}) \\ = \sup_{\varepsilon > 0, \delta > 0} \mu(\{X \in 2^\omega : |g(X) - a| < r - \varepsilon\}) - \delta \end{aligned}$$

where  $g$  depends on  $\varepsilon$  and  $\delta$ . Finally, recall that  $\mu(\{X \in 2^\omega : |g(X) - a| < r - \varepsilon\})$  is lower semicomputable from  $a, r$ . Using this we can approximate  $\mu(\{X \in 2^\omega : |f(X) - a| < r\})$  from below.  $\square$

The following lemma will be the key to this paper.

**Lemma 2.5** (Key Lemma). *Let  $t$  be a lower semicomputable function with a computable integral  $\int t d\mu$ . There is a uniformly computable sequence  $\langle h_n \rangle$  of total computable functions  $h_n : 2^\omega \rightarrow [0, \infty)$  such that  $h_n \leq t$  everywhere and if  $A$  is Schnorr random, there is some  $n$  such that  $h_n(A) = t(A)$ .*

*Proof.* Let  $\langle g_k \rangle$  be a code for  $t$ , namely a sequence of total nonnegative computable functions such that  $t = \sum_k g_k$ . Find a sequence  $\langle f_n \rangle$  of partial sums  $f_n = \sum_{k < k_n} g_k$  (where  $\langle k_n \rangle$  is increasing) such that  $\int (t - f_n) d\mu < 2^{-2n}$ . (This can be done since  $\int g_n d\mu$  is uniformly computable from  $n$ .) By Chebeshev's inequality, for any  $c > 0$ ,

$$\mu(\{X \in 2^\omega : t(X) - f_n(X) > c\}) \leq 2^{-2n}/c.$$

Moreover, we have this claim.

**Claim.** *There is a computable sequence  $\langle c_n \rangle$  such that  $2^{-(n+1)} < c_n < 2^{-n}$  for each  $n$  and  $\mu(\{X \in 2^\omega : t(X) - f_n(X) > c_n\})$  is uniformly computable from  $n$ .*

*Proof of claim.* First, we show that  $t$  is  $L^1$ -computable. Just find  $n_k$  such that  $\|t - f_{n_k}\|_{L^1} = \int (t - f_{n_k}) d\mu < 2^{-k}$ . This is possible since  $\int t d\mu$  is computable.

Now, fix  $n$ . Our goal is to find  $c_n$ . Since,  $t$  is  $L^1$ -computable, so is  $t - f_n$ . Let  $\nu$  to be the distribution of  $t - f_n$ . By Proposition 2.4,  $\nu$  is a computable distribution.

Hence for any real  $c$ ,

$$\mu(\{X \in 2^\omega : t(X) - f_n(X) > c\}) = \nu((c, \infty))$$

is lower semicomputable and

$$\mu(\{X \in 2^\omega : t(X) - f_n(X) \geq c\}) = \nu([c, \infty)) = 1 - \nu((-\infty, c))$$

is upper semicomputable.

It is enough to find some  $c$  in the desired interval such that

$$\mu(\{X \in 2^\omega : t(X) - f_n(X) = c\}) = \nu(\{c\}) = 0.$$

Indeed, the set of all  $c$  such that  $\nu(\{c\}) = 0$  is a computable intersection of dense  $\Sigma_1^0$  sets. Hence by the effective proof of the Baire category theorem (a basic diagonalization argument, see for example [1]), one can effectively

find  $c_n$  in the desired interval such that  $\mu(\{X \in 2^\omega : t(X) - f_n(X) > c_n\})$  is computable. This proves the claim.  $\square$

To define  $h_m$ , replace each  $f_n$  (for  $n > m$ ) with

$$h_n^m = \min(f_n, f_{n-1} + 2^{-(n-1)}, \dots, f_m + 2^{-m}).$$

Define  $h_m = \sup_{n>m} h_n^m$ . For each  $X$  and  $n > m$  we have  $|h_m(X) - h_n^m(X)| \leq 2^{-n}$ . So  $h_m(X)$  is uniformly computable from  $X$  and  $m$ . Also,  $h_m \leq t$  everywhere, and  $t(X) > h_m(X)$  if and only if  $t(X) > f_n(X) + 2^{-n}$  for some  $n > m$ . Then

$$\begin{aligned} \{X \in 2^\omega : h_m(X) > t(X)\} &\subseteq \bigcup_{n>m} \{X \in 2^\omega : t(X) - f_n(X) > 2^{-n}\} \\ &\subseteq \bigcup_{n>m} \{X \in 2^\omega : t(X) - f_n(X) > c_n\} =: U_m. \end{aligned}$$

Notice  $\mu(U_m) \leq \sum_{n>m} 2^{-(n+1)} = 2^{-m}$ , and further  $\mu(U_m)$  is uniformly computable from  $m$ . Hence  $\langle U_m \rangle$  is a Schnorr test.

Finally, for any Schnorr random  $A$ , there is some  $m$  such the  $A \notin U_m$ . Hence  $h_m(A) = t(A)$ .  $\square$

*Remark 2.6.* Notice, this proof gives a uniform algorithm for converting the codes for  $t$  and  $\int t d\mu$  into a code for a Schnorr test  $\langle U_m \rangle$  such that  $t(X)$  is finite when  $X \notin \bigcap_m U_m$ . However, the uniformity is not (and cannot be) independent of the codes. Indeed even a different code for  $\int t d\mu$  can change the sequences  $\langle g_k \rangle$  and  $\langle c_n \rangle$  in the proof leading to a different Schnorr test  $\langle U_m \rangle$ .

As a corollary, we get another proof of Miyabe's characterization of Schnorr randomness via Schnorr integral tests.

**Definition 2.7.**

- (1) An **integral test** is a lower semicomputable function  $t: 2^\omega \rightarrow [0, \infty]$  such that  $\int t d\mu < \infty$ .
- (2) (Miyabe [8]) A **Schnorr integral test** is an integral test  $t$  such that  $\int t d\mu$  is computable.

**Proposition 2.8** (See for example [2]).  *$X$  is Martin-Löf random if and only if there is no integral test  $t$  such that  $t(X) = \infty$ .*

**Corollary 2.9.** *If  $t$  is a Schnorr integral test and  $A$  is Schnorr random, then  $t(A)$  is finite and computable from  $A$ .*

*Proof.* By Lemma 2.5, there is some total computable  $h_n$  such the  $t(A) = h_n(A)$ .  $\square$

**Corollary 2.10** (Miyabe [8]).  *$X$  is Schnorr random if and only if there is no Schnorr integral test  $t$  such that  $t(X) = \infty$ .*

*Proof.* ( $\Rightarrow$ ) Assume  $A$  is Schnorr random and  $t$  is a Schnorr test. By Lemma 2.5, there is some total computable  $h_n$  such the  $t(A) = h_n(A) < \infty$ . ( $\Leftarrow$ ) Assume  $A$  is not Schnorr random by the Schnorr test  $\langle U_n \rangle$ . Then let  $t = \sum_n \mathbf{1}_{U_n}$  where  $\mathbf{1}_{U_n}$  is the characteristic function of  $U_n$ .  $\square$

### 3. VAN LAMBALGEN FOR SCHNORR RANDOMNESS

As a warm up, we use the results from the previous section to give a simple proof of the “ $\Leftarrow$ ” direction of van Lambalgen’s theorem for Schnorr randomness. While our proof is simple, we argue that it is not a straightforward modification of van Lambalgen’s theorem. (Franklin and Stephan [4] also recently gave a very different proof of this result.)

**Theorem 3.1.** *If  $A$  is Schnorr random and  $B$  is Schnorr random relative to  $A$  then  $A \oplus B$  is Schnorr random.*

*Proof.* Assume  $A \oplus B$  is not Schnorr random and that  $A$  is Schnorr random. There is some Schnorr integral test  $t$  such that  $t(A \oplus B) = \infty$ . We wish to show that  $B$  is not Schnorr random relative to  $A$ . For each  $X$ , define  $t^X(Y) = t(X \oplus Y)$ . Clearly,  $t^A(B) = t(A \oplus B) = \infty$ .

We will show that  $t^A$  is a Schnorr integral test relative to  $A$ . For each  $X$ , the function  $t^X$  is lower semicomputable with a code uniformly computable from  $X$ . Define,  $u(X) = \int t^X(Y) d\mu(Y)$ . Notice  $u$  is lower semicomputable and by Fubini’s Theorem

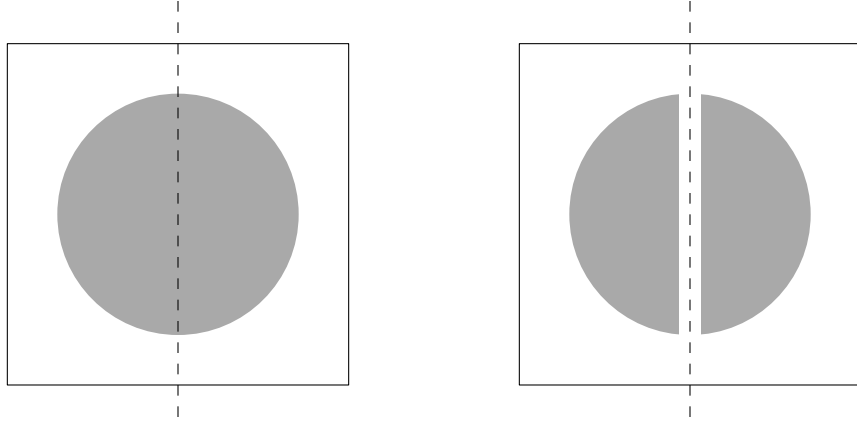
$$\int u(X) d\mu(X) = \iint t(X \oplus Y) d\mu(Y) d\mu(X) = \int t d\mu$$

which is computable. It follows that  $u$  is a Schnorr integral test. Since  $A$  is Schnorr random, by Corollary 2.9,  $u(A)$  is computable from  $A$ , and therefore so is  $\int t^A(Y) d\mu(Y) = u(A)$ . Hence  $t^A$  is a Schnorr integral test relative to  $A$ , and  $B$  is not Schnorr random relative to  $A$ .  $\square$

*Remark 3.2.* Notice the emphasized line in the above proof. The key difficulty in adapting the standard (integral test) proof of van Lambalgen’s theorem to Schnorr randomness is that for Martin-Löf randomness one need only show that  $\int t^A(Y) d\mu(Y)$  is *finite* while here we must show it is *computable from  $A$* . The same difficulties exist when trying to adapt a proof using Martin-Löf tests; given a Schnorr test  $\langle U_n \rangle$  one must show the measure of  $U_n^A := \{Y \in 2^\omega : A \oplus Y \in U_n\}$  is computable from  $A$ .

Consider this latter case. One may incorrectly think that  $\mu(U_n^A)$  is uniformly computable from  $A$ , the code for  $U_n$ , and the measure  $\mu(U_n)$ .<sup>1</sup> This is false, as the following picture shows. The two open sets depicted (on  $2^\omega \times 2^\omega$ ) are almost the same except one contains a small gap. Such a small gap could significantly change the value of  $\mu(U_n^A)$ . It is impossible to determine in a fixed number of steps whether such a small gap exists.

<sup>1</sup>Indeed, this was the error in [9] when proving van Lambalgen’s theorem for truth-table Schnorr randomness.



However, the Key Lemma does show that  $\mu(U_n^A)$  is computable from  $A$  if  $A$  is Schnorr random. One could say such a function is “nearly computable,” i.e. it is computable outside an arbitrary small set. This is an effectivization of Littlewood’s “three principles” of measure theory, particularly Lusin’s theorem which says that a measurable function is “nearly continuous”. It is also the basis behind the layerwise-computability framework of Hoyrup and Rojas [5] and its extensions to Schnorr randomness. (See also [8, 11, 12].)

#### 4. UNIFORMLY RELATIVE SCHNORR RANDOMNESS

In this section we give the correction to Miyabe’s proof of van Lambalgen’s theorem for uniformly relative Schnorr randomness. But first, we define uniformly relative Schnorr randomness.

Recall, that a Schnorr test can be encoded by a function  $f \in \mathbb{N}^{\mathbb{N}}$  which encodes a prefix-free listing of the basic sets in  $U_n$  and encodes a fast Cauchy sequence of rationals converging to each measure  $\mu(U_n)$ . (Recall, a sequence of rationals  $\langle q_n \rangle$  is **fast-Cauchy** if for all  $n \geq m$ , we have  $|q_n - q_m| \leq 2^{-m}$ .)

**Definition 4.1.** A *uniform Schnorr test* is a total computable map  $\Phi: 2^\omega \rightarrow \mathbb{N}^{\mathbb{N}}$  such that each  $\Phi(X)$  encodes a Schnorr test. Also, call a collection  $\langle U_n^X \rangle_{n \in \mathbb{N}, X \in 2^\omega}$  a *uniform Schnorr test* if it is given by a map  $\Phi: 2^\omega \rightarrow \mathbb{N}^{\mathbb{N}}$  as above.

**Definition 4.2** (Miyabe [9], following Franklin and Stephan [3]). Let  $A, B \in 2^\omega$ . Say  $A$  is **Schnorr random uniformly relative to  $B$**  if there is no *uniform Schnorr test*  $\langle U_n^X \rangle_{n \in \mathbb{N}, X \in 2^\omega}$  such that  $A \in \bigcap_n U_n^B$ .

*Remark 4.3.* Uniformly relative Schnorr randomness has previously been called “truth-table Schnorr randomness”. Note that for a sequence  $\langle V_n \rangle$  of open sets, saying that  $V_n = U_n^X$  for some uniform Schnorr test  $\langle U_n^X \rangle_{n \in \mathbb{N}, X \in 2^\omega}$  is not the same (or not obviously the same) as saying that the code for  $\langle U_n \rangle$  is truth-table computable from  $X$ . See Section 6 for more discussion.

Also, it is possible to define uniform tests of other types similarly.

**Definition 4.4.** A *uniform Schnorr integral test* is a total computable map  $\Phi: 2^\omega \rightarrow \mathbb{N}^\mathbb{N}$  such that each  $\Phi(X)$  encodes a Schnorr integral test. Also, call a collection  $\langle t^X \rangle_{X \in 2^\omega}$  a *uniform Schnorr integral test* if it is given by a map  $\Phi: 2^\omega \rightarrow \mathbb{N}^\mathbb{N}$  as above.

**Proposition 4.5.** *Let  $A, B \in 2^\omega$ . Then  $A$  is Schnorr random uniformly relative to  $B$  if and only if there is no uniform Schnorr integral test  $\langle t^X \rangle_{X \in 2^\omega}$  such that  $t^B(A) = \infty$ .*

*Proof.* Follow the proof of Corollary 2.10. The proof is uniform in that the code for one test is computable from the code for the other (see Remark 2.6).  $\square$

*Remark 4.6.* While the reader should not confuse our definition of uniform test with that of Levin [6], the two ideas are closely related. The main difference is that in Levin's definition the uniform test is indexed by probability measures  $\xi$  and the test  $t^\xi$  was with respect to the measure  $\xi$  (i.e.  $\int t^\xi d\xi < \infty$ ).

Now, we prove the main result. The proof will closely follow that of Theorem 3.1, but will use the full power of the Key Lemma (Lemma 2.5).

**Theorem 4.7.**  *$A \oplus B$  is Schnorr random if and only if  $A$  is Schnorr random and  $B$  is Schnorr random uniformly relative to  $A$ .*

*Proof.* ( $\Rightarrow$ ) This direction is correctly proved in [9].

( $\Leftarrow$ ) Assume  $A \oplus B$  is not Schnorr random and that  $A$  is Schnorr random. There is some Schnorr integral test  $t$  such that  $t(A \oplus B) = \infty$ . We wish to show that  $B$  is not Schnorr random uniformly relative to  $A$ . For each  $X$ , define  $t^X(Y) = t(X \oplus Y)$ . Clearly,  $t^A(B) = t(A \oplus B) = \infty$ .

While  $\langle t^X \rangle_{X \in 2^\omega}$  may not be a uniform Schnorr integral test, we will construct a uniform Schnorr integral test  $\langle \hat{t}^X \rangle_{X \in 2^\omega}$  such that  $\hat{t}^A = t^A$ . For each  $X$ , the function  $t^X$  is lower semicomputable with a code uniformly computable from  $X$ . Define,  $u(X) = \int t^X(Y) d\mu(Y)$ . Notice  $u$  is lower semicomputable and by Fubini's theorem

$$\int u(X) d\mu(X) = \iint t(X \oplus Y) d\mu(Y) d\mu(X) = \int t d\mu$$

which is computable. It follows that  $u$  is a Schnorr integral test. By the Key Lemma (Lemma 2.5), there is some total computable function  $h \leq u$  such that  $u(A) = h(A)$ . Let  $\hat{t}^X$  be  $t^X$ , but enumerated only so that  $\int \hat{t}^X d\mu = h(X)$ . More formally, for  $X$  let  $\langle g_n^X \rangle$  be the code for  $t$ , namely the sequence of total nonnegative computable functions such that  $t^X = \sum_n g_n^X$ . Label the integrals of the partial sums  $c_n^X = \int \sum_{k < n} g_k^X d\mu$ . Define

$$\hat{t}^X = \sum_n \begin{cases} g_n^X & \text{if } c_{n+1}^X < h(X) \\ \left( \frac{h(X) - c_{n+1}^X}{c_{n+1}^X - c_n^X} \right) \cdot g_n^X & \text{if } c_n \leq h(X) \leq c_{n+1}^X \\ 0 & \text{if } h(X) < c_n \end{cases}$$



Then  $\langle \hat{t}^X \rangle_{X \in 2^\omega}$  is a uniform Schnorr integral test where  $\int \hat{t}^X d\mu = h(X)$  and if  $h(X) = u(X)$  then  $\hat{t}^X = t^X$ . Since  $h(A) = u(A)$ , we have  $\hat{t}^A(B) = t^A(B) = \infty$ . Therefore  $B$  is not Schnorr random uniformly relative to  $A$ .  $\square$

## 5. UNIFORMLY RELATIVE COMPUTABLE RANDOMNESS

In this section we give a weaker version of van Lambalgen's theorem for uniformly relative computable randomness.

Recall that a ***martingale*** is a function  $d: 2^{<\omega} \rightarrow [0, \infty)$  such that  $d(\sigma 0) + d(\sigma 1) = 2d(\sigma)$  for all  $\sigma \in 2^{<\omega}$ . We will say a martingale  $d$  ***succeeds*** on a set  $A \in 2^\omega$  if  $\limsup_n d(A \upharpoonright n) = \infty$ . A set  $A$  is ***computably random*** (or ***recursively random***) if there is no computable martingale  $d$  which succeeds on  $A$ . A well-known alternate characterization is that  $A$  is computably random if and only if there is no computable martingale  $d$  such that  $\lim_n d(A \upharpoonright n) = \infty$ .

**Definition 5.1.** A ***uniform martingale test*** is a total computable map  $\Phi: 2^\omega \rightarrow \mathbb{N}^\mathbb{N}$  such that each  $\Phi(X)$  encodes a martingale. Also, call a collection  $\langle d^X \rangle_{X \in 2^\omega}$  a ***uniform martingale test*** if it is given by a map  $\Phi: 2^\omega \rightarrow \mathbb{N}^\mathbb{N}$  as above.

**Definition 5.2** (Miyabe [9]).  $A$  is ***computably random uniformly relative to  $B$***  if there is no uniform martingale test  $\langle d^X \rangle_{X \in 2^\omega}$  such that  $d^B$  succeeds on  $A$ .

Uniformly relative computable randomness was previously called “truth-table reducible randomness” in [9]. In Section 6 we give an alternative definition using truth-table reducibility in the spirit of Franklin and Stephan.

The first author [9] claimed the following, but the proof of the “ $\Leftarrow$ ” direction is incorrect.<sup>2</sup>

$A \oplus B$  is computably random if and only if  $A$  is computably random and  $B$  is computably random uniformly relative to  $A$ .

However, we can prove this weaker version of van Lambalgen's theorem for uniformly relative computable randomness.

<sup>2</sup>The logical error in [9, Theorem 5.10] is in the following formula.

$$\mu(\{Y \mid A \oplus Y \in W_n\} \cap [\tau]) \leq \frac{\nu(A \upharpoonright m \oplus \tau)}{\nu(A \upharpoonright m \oplus \lambda)} 2^{-n}$$

The first  $A$  should be  $[A \upharpoonright m]$  and the  $\in$  should be  $\subseteq$ . Then the next line about letting  $m = 0$  does not hold.

The conceptual error is as follows. The proof as usual starts by assuming  $A \oplus B$  is not computably random. The witnessing test is a bounded Martin-Löf test with bounding measure  $\nu$ . The proof attempts to show that the bounding measure  $\tau \mapsto \nu(\lambda \oplus \tau)$  (where  $\lambda$  is the empty string) witnesses that  $B$  is truth-table reducibly random relative to  $A$ . However,  $\tau \mapsto \nu(\lambda \oplus \tau)$  (that is, the marginal distribution of the second coordinate) is computable (not just computable relative to  $A$ ). Hence this argument would show that  $B$  is not computably random, which is too strong.

**Theorem 5.3.**  *$A \oplus B$  is computably random if and only if  $A$  is computably random uniformly relative to  $B$  and  $B$  is computably random uniformly relative to  $A$ .*

Before giving the formal proof, we give the main idea. Assume some computable martingale  $d$  satisfies  $\lim_n d((A \oplus B) \upharpoonright n) = \infty$ . Then split  $d$  into two martingales  $d_0^B$  and  $d_1^A$ . Here  $d_0^B$  uses  $B$  to bet on the  $n$ th bit of some set  $X$  with the same relative amount that  $d$  bets on the  $2n$ th bit of  $X \oplus B$ . The martingale  $d_1^A$  is defined similarly. We will show  $d((A \oplus B) \upharpoonright 2n) = d_0^B(A \upharpoonright n) \cdot d_1^A(B \upharpoonright n)$ . So either  $d_0^B$  succeeds on  $A$  or  $d_1^A$  succeeds on  $B$ .

To prove the theorem, we introduce the following notation. Given a martingale  $d$  such that  $d(\sigma) \neq 0$  for all  $\sigma \in 2^{<\omega}$ , define  $\tilde{d}(\sigma i) = \frac{d(\sigma i)}{d(\sigma)}$  for  $i \in \{0, 1\}$ . This codes the martingale by the relative changed at each step. The martingale can be recovered by  $d(\sigma) = \prod_{m=1}^{|\sigma|} \tilde{d}(\sigma \upharpoonright m)$  (assuming  $d(\emptyset) = 1$ ). Also  $\tilde{d}$  codes a martingale if and only if  $\tilde{d}(\sigma 0) + \tilde{d}(\sigma 1) = 2$  for all  $\sigma$ . Call  $\tilde{d}$  the **multiplicative representation** of the martingale  $d$ .

Another notion will be as follows. If  $\sigma, \tau \in 2^{<\omega}$ , then define  $f = \sigma \oplus \tau$  as a partial function from  $\mathbb{N}$  to  $\{0, 1\}$  such that  $f(2n) = \sigma(n)$  if  $n < |\sigma|$  and  $f(2n+1) = \tau(n)$  if  $n < |\tau|$ .

*Proof of Theorem 5.3.* Assume  $A \oplus B$  is not computably random. Then there is a computable martingale  $d$  such that  $\lim_n d((A \oplus B) \upharpoonright n) = \infty$ . (Without loss of generality,  $d(\emptyset) = 1$  and  $d(\sigma) > 0$  for all  $\sigma$ .) Define two uniform martingale tests  $\langle d_0^X \rangle_{X \in 2^\omega}$  and  $\langle d_1^X \rangle_{X \in 2^\omega}$  by their corresponding multiplicative representations as follows.

$$\begin{aligned}\tilde{d}_0^Y(\sigma) &= \tilde{d}(\sigma \oplus (Y \upharpoonright |\sigma| - 1)) \\ \tilde{d}_1^X(\tau) &= \tilde{d}((X \upharpoonright |\tau|) \oplus \tau)\end{aligned}$$

Then  $\tilde{d}_0^Y$  (and similarly  $\tilde{d}_1^X$ ) is a multiplicative martingale since

$$\tilde{d}_0^Y(\sigma 0) + \tilde{d}_0^Y(\sigma 1) = \tilde{d}((\sigma \oplus (Y \upharpoonright |\sigma|))^{\wedge} 0) + \tilde{d}((\sigma \oplus (Y \upharpoonright |\sigma|))^{\wedge} 1) = 2.$$

Now for  $X = A$  and  $Y = B$  we have that

$$\begin{aligned}d_0^B(A \upharpoonright n) \cdot d_1^A(B \upharpoonright n) &= \left( \prod_{m=1}^n \tilde{d}_0^B(A \upharpoonright m) \right) \cdot \left( \prod_{m=1}^n \tilde{d}_1^A(B \upharpoonright m) \right) \\ &= \prod_{m=1}^{2n} \tilde{d}((A \oplus B) \upharpoonright m) \\ &= d((A \oplus B) \upharpoonright 2n) \rightarrow \infty\end{aligned}$$

Then either  $d_0^B$  succeeds on  $A$  or  $d_1^A$  succeeds on  $B$ . It follows that one of  $A, B$  is not computably random uniformly relative to the other.  $\square$

We also obtain this easy corollary. Since it follows from the “ $\Rightarrow$ ” direction of Theorem 5.3, it was provable from the results of [9].

**Corollary 5.4.** *There exist sets  $A$  and  $B$  such that  $A$  is computably random uniformly relative to  $B$ , but  $A$  is not computably random relative to  $B$ .*

*Proof.* Merkle et al. [7] showed that there are two computable randoms  $A, B$  such that  $A \oplus B$  is computably random, but  $A$  is not computably random relative to  $B$ . However, by Theorem 5.3,  $A$  is computably random uniformly relative to  $B$ .  $\square$

**5.1. Remark on Kolmogorov-Loveland and Martin-Löf randomness.** Recall that Kolmogorov-Loveland randomness is a notion of randomness similar to computable randomness, except the martingales do not need to bet on the bits in order. These are called **nonmonotonic martingales**. Also, the martingales may be **partial**, i.e. not defined on all inputs. (See [7, 2, 10] for formal definitions and more information on Kolmogorov-Loveland randomness.) The proof of Theorem 5.3 is similar to the proof of the following.

**Theorem 5.5** (Merkle et al. [7]).  *$A \oplus B$  is Kolmogorov-Loveland random if and only if  $A$  and  $B$  are Kolmogorov-Loveland random relative to each other.*

One may ask if there is a notion of “uniformly relative Kolmogorov-Loveland randomness” using uniform partial nonmonotonic martingale tests. The answer is that being Kolmogorov-Loveland random uniformly relative to  $B$  is the same as being Kolmogorov-Loveland random relative to  $B$ . Any nonmonotonic martingale computable from  $B$ , is easily extended to a uniform partial nonmonotonic martingale. This is easy to do because the nonmonotonic martingale needs only be partial computable from the oracle.

Similarly, “Martin-Löf random uniformly relative to  $B$ ” is equivalent to Martin-Löf random relative to  $B$ . If  $\langle U_n \rangle$  is a Martin-Löf test relative to  $B$ , then there is a uniform Martin-Löf test  $\langle U_n^X \rangle_{n \in \mathbb{N}, X \in 2^\omega}$  given by using the same algorithm (as for  $\langle U_n \rangle$ ) to enumerate the basic open sets of  $U_n^X$ , but we stop enumerating the basic open sets if doing so will make  $\mu(U_n^X) > 2^{-n}$ .

## 6. TRUTH-TABLE SCHNORR AND TRUTH-TABLE REDUCIBLE RANDOMNESS

Truth-table Schnorr randomness was first defined by Franklin and Stephan [3] as follows using a truth-table relativized martingale test. Recall that a function  $f \in \mathbb{N}^\mathbb{N}$  is **truth-table reducible** to  $A \in 2^\omega$  if there is a total computable functional  $\Phi: 2^\omega \rightarrow \mathbb{N}^\mathbb{N}$  such that  $f = \Phi(A)$ .

**Definition 6.1** (Franklin and Stephan [3]). A set  $A$  is **truth-table Schnorr relative to  $B$**  if there is no martingale  $d$  whose code is truth-table reducible to  $A$ , and no function  $f: \mathbb{N} \rightarrow \mathbb{N}$  truth-table reducible to  $B$  such that  $\exists^\infty n [d(A \upharpoonright f(n)) \geq n]$ .

Franklin and Stephan also remark that one may take  $f$  in the above definition to be computable (instead of truth-table reducible to  $B$ ) with no loss.

The first author showed in [9] that truth-table Schnorr randomness is equivalent to (what we call) uniformly relative Schnorr randomness, but there was a small gap in the proof which we feel would be instructive to fill in here.

**Lemma 6.2.** *Let  $d$  be a martingale (whose code is) truth-table reducible to  $A$  and let  $f: \mathbb{N} \rightarrow \mathbb{N}$  be truth-table reducible to  $A$ . Then there is a uniform martingale test  $\langle \hat{d}^X \rangle_{X \in 2^\omega}$  and a uniform function  $\langle \hat{f}^X \rangle_{X \in 2^\omega}$  such that  $\hat{d}^A = d$  and  $\hat{f}^A = f$ .*

*Proof.* Let  $d$  be a martingale truth-table reducible to  $A$ . And let  $\Phi: 2^\omega \times 2^{<\omega} \rightarrow \mathbb{N}^\mathbb{N}$  be a total computable functional such that  $\Phi(A, \sigma)$  encodes the fast-Cauchy code for  $d(\sigma)$ . Define  $d^X(\sigma)$  to be the real coded by  $\Phi(X, \sigma)$ . Note, that there is no guarantee that, first,  $\Phi(X, \sigma)$  is a Cauchy code for a non-negative real for every  $X$  and  $\sigma$ , and that, second,  $d^X$  is a martingale for every  $X$ .

The first issue is easily fixed. A folklore trick is that  $\Phi(X, \sigma)$  can be forced to be a fast Cauchy code. Let  $\langle q_0, q_1, \dots \rangle$  be the sequence of rationals given by  $\Phi(X, \sigma)$ . Find the first  $n$ , if any, such that  $|q_n - q_m| > 2^{-m}$  for  $m \leq n$ , then change the code to be  $\langle q_0, q_1, \dots, q_{n-1} \rangle \hat{\ } \langle q_{n-1}, q_{n-1} \dots \rangle$ . Also do the same trick if  $q_n < 0$ .

The second issue is also easily handled. Assuming, now that each  $d^X(\sigma)$  is a nonnegative real, define  $\hat{d}^X(\sigma)$  by recursion as follows.

$$\begin{aligned} \hat{d}^X(\emptyset) &= d^X(\emptyset) \\ \hat{d}^X(\sigma 0) &= \min(d^X(\sigma 0), 2\hat{d}^X(\sigma)) \\ \hat{d}^X(\sigma 1) &= 2\hat{d}^X(\sigma) - \hat{d}^X(\sigma 0) \end{aligned}$$

It is easy to check  $\hat{d}^X$  is a martingale whose code is uniformly computable from the code for  $d^X$ . Also if  $d^X$  is already a martingale, then  $\hat{d}^X = d^X$ . In particular,  $\hat{d}^A = d^A$ .

Last if  $f$  is truth-table reducible to  $A$ , then there is a total functional  $\Psi: 2^\omega \times \mathbb{N}^\mathbb{N} \rightarrow \mathbb{N}^\mathbb{N}$  such that  $\Psi(A) = f$ . Define  $\hat{f}^X = \Psi(X)$ .  $\square$

*Remark 6.3.* Notice the motivation behind Definition 6.1 is to say that  $A$  is “truth-table Schnorr random” relative to  $B$  if there is no test for Schnorr randomness (e.g. Schnorr test, integral test, martingale test, etc.) which is truth-table reducible to  $B$  and witnesses that  $A$  is not random for that test. Unfortunately, this method is very sensitive to the choice of test. Lemma 6.2 does not seem to hold for most other characterizations of Schnorr randomness, including the usual martingale characterization. Indeed, the usual martingale characterization (see for example [2]) involves an order, i.e. a computable, nondecreasing, unbounded function  $f: \mathbb{N} \rightarrow \mathbb{N}$ . It is not in general possible to extend an order  $f$  truth-table reducible to  $A$  to a uniform order  $\langle f^X \rangle_{X \in 2^\omega}$ . To do this, one would also need that the rate of growth of  $f$  is truth-table reducible to  $A$ . A similar phenomenon happens

with Schnorr tests. One needs not only that the measure of  $\mu(U_n)$  is truth-table reducible to  $A$ , but also that if  $U_n$  is coded by the prefix-free set  $\{\sigma_n\}$ , then the rate of convergence of  $\sum_{k \leq n} \mu(\sigma_k)$  is truth-table reducible to  $A$ . (Also see Franklin and Stephan [3, Theorem 2.2] for a related discussion.)

Now we can show that the definitions are equivalent.

**Proposition 6.4.** *A set  $A$  is Schnorr uniformly relative to  $B$  if and only if  $A$  is truth-table Schnorr relative to  $B$ .*

*Proof.* By Lemma 6.2 (and its trivial converse) truth-table Schnorr randomness is equivalent to that obtained from uniform martingale tests of the above type. Now similar to Proposition 4.5, it is enough to show a uniform martingale test (of the above type) can effectively be converted to a Schnorr test which covers the same points that the martingale succeeds on, and vice versa. Indeed, the proofs in the literature are effective in this regard (see [3, 2, 10]).  $\square$

*Remark 6.5.* There is an important subtlety in the last proof similar to Remark 2.6. We showed it is possible to compute *the code* for one test from *the code* of another test uniformly. However, it is not necessarily possible to do so in a way that is independent of the choice of codes. For example, it is known that one may effectively replace a real-valued martingale  $d$  with a rational-valued martingale  $\hat{d}$  that succeeds on the same points. However, there is some  $d$  such that different codes for  $d$  lead to different rational approximations. This will become an issue if instead of relativizing with respect to a set  $X \in 2^\omega$ , one relativizes with respect to a real  $x \in [0, 1]$ .

We also have a similar result for computable randomness.

**Proposition 6.6.** *A set  $A$  is computably random uniformly relative to  $B$  if and only if for all martingales  $d$  (whose codes are) truth-table reducible to  $B$ , we have that  $\limsup_n d(A \upharpoonright n) < \infty$ .*

*Proof.* By the proof of Lemma 6.2 it is possible to pass from a martingale truth-table reducible to  $B$  to a uniform martingale test. The converse is trivial.  $\square$

Hence, uniformly relative computable randomness is also known as **truth-table reducible randomness** [9].

## REFERENCES

- [1] Vasco Brattka. Computable versions of Baire's category theorem. In *Mathematical foundations of computer science, 2001 (Mariánské Lázně)*, volume 2136 of *Lecture Notes in Comput. Sci.*, pages 224–235. Springer, Berlin, 2001.
- [2] Rodney G. Downey and Denis R. Hirschfeldt. *Algorithmic randomness and complexity*. Theory and Applications of Computability. Springer, New York, 2010.
- [3] Johanna N. Y. Franklin and Frank Stephan. Schnorr trivial sets and truth-table reducibility. *J. Symbolic Logic*, 75(2):501–521, 2010.

- [4] Johanna N. Y. Franklin and Frank Stephan. Van Lambalgen's theorem and high degrees. *Notre Dame J. Form. Log.*, 52(2):173–185, 2011.
- [5] Mathieu Hoyrup and Cristóbal Rojas. An application of Martin-Löf randomness to effective probability theory. In *Mathematical theory and computational practice*, volume 5635 of *Lecture Notes in Comput. Sci.*, pages 260–269. Springer, Berlin, 2009.
- [6] L. A. Levin. Uniform tests for randomness. *Dokl. Akad. Nauk SSSR*, 227(1):33–35, 1976.
- [7] Wolfgang Merkle, Joseph S. Miller, André Nies, Jan Reimann, and Frank Stephan. Kolmogorov-Loveland randomness and stochasticity. *Ann. Pure Appl. Logic*, 138(1-3):183–210, 2006.
- [8] Kenshi Miyabe.  $L^1$ -computability and layerwise computability. *In preparation*.
- [9] Kenshi Miyabe. Truth-table Schnorr randomness and truth-table reducible randomness. *MLQ Math. Log. Q.*, 57(3):323–338, 2011.
- [10] André Nies. *Computability and randomness*, volume 51 of *Oxford Logic Guides*. Oxford University Press, Oxford, 2009.
- [11] Noopur Pathak, Cristóbal Rojas, and Stephen G. Simpson. Schnorr randomness and the Lebesgue differentiation theorem. *Proceedings of the American Mathematical Society*, To appear.
- [12] Jason Rute. Algorithmic randomness, martingales, and differentiability I. *In preparation*.
- [13] Michiel van Lambalgen. The axiomatization of randomness. *J. Symbolic Logic*, 55(3):1143–1167, 1990.
- [14] Liang Yu. When van Lambalgen's theorem fails. *Proc. Amer. Math. Soc.*, 135(3):861–864, 2007.